ECO
Verband der deutschen Internetwirtschaft

Arbeitskreis WLAN
AG Sicherheit

Statusbericht

Patrick Postel / datenaura.com
Holger Zuleger / Arcor AG

Zielsetzung AG-Sicherheit

- Erstellen von Sicherheitsempfehlungen bzw. Richtlinien für
  - Hotspot Betreiber
  - Hotspot Nutzer
  - Hotspot Roamingpartner (Clearinghouse)
- Keine Aussagen bezüglich der Nutzung der WLAN Technik
  - im privaten Bereich
  - im Firmenumfeld

  Für beide Nutzungsarten existiert eine Empfehlung des Bundesamtes für Sicherheit in der Informationsverarbeitung (BSI).

  Schwerpunkt der Arbeit des AK-WLAN liegt auf Public Hotspots.

Datensicherheit bei Wireless Hotspots

- Authentisierung
  - Sollte immer beidseitig stattfinden (mutual authentication).
  - Die Authentisierungsdaten sollten verschlüsselt übertragen werden.
  - Grundlage für Datenintegrität, Accounting und Verschlüsselung.
- Datenintegrität
  - Gewährleistet die Zuordnung der Datenpakete zu einem authentisierten Nutzer.
  - Verhindert Sessionübernahme durch Angreifer.
  - Gewährleistet korrektes Accounting.
  - Setzt Nutzerauthentisierung voraus.

Datensicherheit bei Wireless Hotspots (2)

- Accounting
  - Zeit- oder volumenbasierte Abrechnung der Session.
  - Setzt Erkennen des Start- und Endezeitpunktes voraus.
    - Ersteres wird durch die Authentisierung gewährleistet.
    - Letzteres über Keepalives bzw. expliziten Verbindungsabbau.
  - Setzt Datenintegrität voraus.
- Verschlüsselung
  - Gewährleistung der Vertraulichkeit der Daten auf der Funkstrecke!
  - Setzt beidseitige Authentifizierung und Datenintegrität voraus.

Authentisierungsverfahren

- Webauthentisierung
  - Sichere Authentisierung über HTTPS.
  - Datenintegrität auf IP-Ebene.
  - Datenverschlüsselung prinzipbedingt nicht möglich.
- IPsec
  - Authentisierungsverfahren für Public Hotspots ungeeignet (shared Secret, Clientzertifikate)
  - Datenintegrität über kryptographische Verfahren.
  - Datenverschlüsselung über kryptographische Verfahren die zur Zeit als absolut sicher gelten.
  - Sessionende gut zu erkennen.

  Empfohlenes Verfahren für Verbindungen mit dem Firmennetzwerk.

Authentisierungsverfahren (2)

- WAP, 802.11i
  - Für Public Hotspots geeignete Authentisierungverfahren (EAP-TTLS oder PEAP).
  - Datenintegrität über kryptographische Verfahren.
  - Datenverschlüsselung für Public Hotspot ausreichend.
  - Zur Zeit keine breite Verfügbarkeit (802.11i erst Ende 2003?).
- PPTP (Point to Point Tunnel Protocol)
  - Sichere Authentisierung über MS-CHAPv2.
  - Datenintegrität über kryptographische Verfahren.
  - Datenverschlüsselung für Public Hotspot ausreichend.
  - Sessionende gut zu erkennen.

Sicherheitsempfehlung für Hotspot Betreiber

- Eingesetzte Sicherheitsverfahren sind zu publizieren (Sicherheitshinweis, Policy).
- Authentifizierungsdaten sollten verschlüsselt übertragen werden.
- Mindestens ein Verfahren zur verschlüsselten Datenübertragung.
  - Nutzung optional (insbes. bei spez. Clientsoftware).
  - Nutzer ist auf die Möglichkeit hinzuweisen.
  - Nutzung ohne zusätzliche Kosten.
- Es sind geeignete Verfahren zur Datenintegrität einzusetzen (Accounting).
- Keine Behinderung des Einsatzes von Verschlüsselungssoftware auf Nutzerseite (NAT, PAT).
- Ergänzung:
  Verwendung von gültigen und signierten Serverzertifikaten.
  Frage: Welche CA? Greenspot?!

Sicherheitsempfehlung für Hotspot Nutzer

Jeder Nutzer muß sich über seine Sicherheitsanforderungen bewußt sein.

Allgemeine Richtlinien sollen ihn dabei unterstützen:

- Nur verschlüsselte Authentisierung an dem Public Hotspot.
- Ergänzung:
  Überprüfung des Serverzertifikats auf Korrektheit (Fingerprint, Ablaufdatum, Zertifizierungsinstanz).
- Nutzung ohne Datenverschlüsselung nur, wenn keinerlei personenbezogenen Daten (Passwörter, Email) übertragen werden.
- Personenbezogene Daten müssen auf Anwendungsebene verschlüsselt werden (HTTPS, POP3+SSL, IMAPS, SMTP/TLS).
- Verschlüsselung auf der Funkstrecke entspricht der Vertraulichkeit einer Internet Dialin-Verbindung.
- Hierbei **kann** auf die Verschlüsselung auf Anwendungsebene verzichtet werden.
- Der Zugriff auf ein Firmennetzwerk sollte **ausschließlich** über IPsec bis zum Security Gateway des Firmennetzwerkes erfolgen.

Sicherheitsempfehlung für Roaming Partner

Alle Angaben sind zur Zeit nicht abgestimmt!

Absprache mit Roaming AG notwendig!

- Nur verschlüsselte Authentisierung an dem Public Hotspot.
- Die Kommunikation zwischen dem Access Gateway und dem Authentisierungssystem sollte verschlüsselt werden wenn die Kommunikation über fremde Netze erfolgt.
- Die Kommunikation zwischen den Roamingpartnern resp. der Clearingstelle **muß** verschlüsselt erfolgen.
- Für die Gewährleistung der Datenintegrität müssen Verfahren jenseits von IP- oder Hardwareadressen eingesetzt werden.
- Die Datenverschlüsselung ist in diesem Zusammenhang nicht von Bedeutung.

ToDo

- Überarbeiten und Verabschieden der Sicherheitsempfehlung.
- Veröffentlichen einer Richtline für die Nutzung von Public Hotspots.
- Weitere Punkte?

ToDo

- Überarbeiten und Verabschieden der Sicherheitsempfehlung.
- Veröffentlichen einer Richtline für die Nutzung von Public Hotspots.
- Weitere Punkte?

? Fragen ?

ToDo

- Überarbeiten und Verabschieden der Sicherheitsempfehlung.
- Veröffentlichen einer Richtline für die Nutzung von Public Hotspots.
- Weitere Punkte?

? Fragen ?

Vielen Dank für ihre Aufmerksamkeit!

CONTENTS